Data processing agreement between Continia customer and Continia Software A/S

VERSION 2.0 OF 15. SEPTEMBER 2021

DATA PROCESSING AGREEMENT

Between
the Continia Customer
(hereinafter referred to as ‘the controller’ or ‘the Customer’)

Customer Name	
Adresss	
Country	
Company registration number	

and
Continia Software A/S
Stigsborgvej 60
9400 Nr. Sundby
Denmark
Company registration (CVR) no.: DK32658083
(hereinafter referred to as ‘the processor’ or ‘Continia’)

Standard contractual clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them. Such add-on or update shall be made and accepted in writing with a notice period of no less than 30 days, except for change of sub-contractors (Clause 7.7) or other material issues, where the notice period shall be 2 months.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented per the instructions specified in Annex III.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II,unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

The Parties shall be able to demonstrate compliance with these Clauses.

(a) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(b) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(c) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(d) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 2 months' notice in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 , with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s):

1. Name:

Business Identification Number (e.g. VAT, CVR, KVK, EIN, HR) if applicable:

Address:

Contact person's:

Name:

Position:

Contact details:

Telephone:

E-mail:

Signature and accession date:

Processor(s):

1. Name: Continia Software A/S

Business Identification Number (e.g. VAT, CVR, KVK, EIN, HR) if applicable: CVR 32658083

Address: Stigsborgvej 60, 9400 Nørresundby, Denmark

Contact person's:

Name: Jens Toftegaard Boesen

Position: Chief of Staff

Contact details: jtb@continia.com or +45 25 36 18 74

Signature and accession date:

Henrik Lærke, CEO

15. September 2021

ANNEX II

2.1. Overall description of the processing

Processing of The Customer’s personal data shall take place in accordance with the purpose in the Main Agreement.

Continia may not use the personal data for other purposes.

This section describes the procedures of Continia’s services and hence the purposes of data to be processed and stored, permanent or temporary, with Continia software and as applicable to the extent relevant in accordance with the Main Agreement.

2.2. Categories of data subjects, whose personal data is processed

I. Employees
II. Suppliers and business partners
III. Users of Software products and Online Services (including employees of the data controller)

2.3 Categories of personal data about the data subjects processed

Re. 2.2. (I): Name, email, expenses, mileage, settlements and related data, corporate credit card expenses and bank statements, vouchers

Re 2.2. (II): Name(s) of suppliers' employee(s), email(s) of suppliers' employee(s), name of data controller's employee(s) (as invoice recipient(s)), and additional information contained in invoices (including services rendered)
If the supplier is a sole proprietorship, types of personal data also include name of owner, address, account no., account reg. no., bank name, IBAN, SWIFT, creditor number, SE-No., P-No., receiver reference

Re 2.2. (III): Dynamics username, Windows username, e-mail address, name, general approval data related to documents for approval and usage data, including approval comments.

2.4 The nature of, purpose and duration of the processing, including specification of the data subjects and personal data handled

2.4.1 Personal Data related to Continia Document Capture

Processing of Data and personal data is necessary to be able to receive and process e-mail and PDF-files. It is not possible precisely to foresee whether the data stored by The Customer will contain personal data as this fully depends on whether this data relates to an “identified or identifiable natural person”. Consequently, when referring to “Data” below, this will automatically include personal data.

Personal data will be stored with Continia only when using Continia Cloud OCR. Otherwise, data will be stored at the Customer and/or the relevant service providers used by the Customer only.

1. Flow
Document categories will be exported to Continia Online Services for Continia Cloud OCR to be able to receive e-mails. This happens as part of the initial configuration or when the user manually exports them.

Documents are sent as attachments in email to unique customer specific e-mail address. The e-mail is received in Amazon Web Services (AWS) Simple Email Service and stored as an EML file. A message, to notify Continia Cloud OCR, is written to an AWS Simple Queue Service queue.

Continia Cloud OCR monitor the AWS queue, when a new e-mail arrives, Continia retrieves and stores the e-mail and PDFs in Continia Online Services.

Continia Cloud OCR sends the PDF to ABBYYs OCR Service and receive the OCR result as XML. The ABBYY OCR service may queue (store) PDFs until processed and store result until retrieved by Continia Cloud OCR.

Continia retrieves the PDF and OCR result from ABBYY OCR Service and stores it in Continia Online Services and sends it to the Customers Business Central when requested by the customer (daily or hourly or manually). After retrieval is completed, it is deleted from Continia Online Services (Azure in Ireland)

2. Expiration
Data will remain stored until downloaded to the customer or will be deleted after 180 days.

3. Content
Data related to document categories, such as Code, Description, Connection Endpoint Code

Personal data related to processed e-mails.
Such as Sender e-mail, Sender name, Subject, Body, all attachments

4. Sensitivity
Personal data of Sender e-mails and Sender names is considered less sensitive.

The content of e-mails and attachments can potentially be personal sensitive but beyond the control or influence of Continia.

2.4.2. Personal Data related to Continia Expense Management

When using Expense Management, there are multiple integration points where data is sent and received from and to NAV/Business Central/Business Central, to Continia Online Services and to the mobile Expense app.

1. Flow
Expense users are synchronized to Continia Online Services to allow them to log in to the app and the Expense Portal.

Master Data from NAV/Business Central is synchronized to Continia Online Services and used when working with expenses and mileage in the app or the Expense Portal.

There are three different ways to process Bank transactions:

1) Bank transactions can be received by Continia Online Services from the bank, on behalf of The Customer. Later, bank transactions are downloaded to the customer and deleted from Continia Online Services.

2) Bank transactions can be downloaded as a file by the customer, directly from the bank. This file is uploaded to Continia Online Services, which will process it and return it immediately to the customer.

3) Bank transactions can be processed by Continia Document Capture with OCR On-Premise or Continia Cloud OCR. Please refer to the section "Data related to Continia Document Capture" for more details.

The expense app downloads data from Continia Online Services and stores it on the device. When a user creates or updates an existing record in the app, then it is automatically sent to Continia Online Services and made available for download to NAV/Business Central.

The Expense Portal hosted by Continia Online Services uses Data already synchronized to Continia Online Services. When a user creates or updates an existing record, then it is automatically updated with Continia Online Services and made available for download to NAV/Business Central and to the app.

2. Expiration

Expense users' Data are stored for 180 days or until removed and exported from NAV/Business Central.

Master Data from NAV/Business Central remain stored until removed in NAV/Business Central or until automatically deleted after a maximum of 180 days and the synchronization routine has run in NAV/Business Central.

Bank transactions received by Continia Online Services from the bank remain stored until the synchronization routine has run in NAV/Business Central or until automatically deleted after 180 days.

All expenses, mileage, settlements and related data are stored with Continia Online Services while Status = "Pending Expense User".

When Status is no longer "Pending Expense User" the Data are removed from Continia Online Services when the synchronization routine has run in NAV/Business Central or until automatically deleted after 180 days.

When expense, mileage or settlement is approved this can trigger an approval notification to the user. Approval notifications are uploaded to Continia Online Services and downloaded to the app when it connects.

Approval notification is removed from Continia Online Services after downloading to the app.
The approval notification is removed from Continia Online Services if not downloaded by the app user within 90 days.

Historical expenses, mileage, and settlements is stored in the app and devices they have been downloaded to.

The user can either delete history manually or configure automatic deletion, i.e. after one month. History is also deleted if the app is un-installed or the phones being reset.

History in the app is not deleted by deleting the user in NAV/Business Central as there is no way to control that the device and app get connected to the internet.

3. Content

Data related to expense users.

Personal Data related to master data.

Such as Expense types, Dimensions, and other configured fields with a look up to a table

Data related to bank transactions such as Card ID, Card name, Date, Amount, Place of purchase.

Data related to expenses. such as User identification, Expense type, Date, Description, Amount.

Data related to mileage, such as User identification, Date, Address where the user was driving from and to

Data related to settlements, such as User identification, Date, associated expenses and mileage

4. Sensitivity

Master data are not considered personal sensitive.

All other Data are considered personal sensitive.

2.4.3 Personal Data related to Continia Web Approval Portal

The Web Approval Portal works in combination with Continia Document Capture and Continia Expense Management. The Web Approval Portal can either be installed On-Premise or hosted with Continia Software. Only when hosted with Continia Software will Data be stored with Continia Online Services.

1. Flow
When a user logs into the Web Approval Portal, Data are processed from NAV/Business Central using NAV/Business Central Web Services. When a user accesses a record for approval, then the primary PDF or JPG for that document is uploaded from NAV/Business Central and displayed to the user.

2. Expiration
Users' Data remain stored until removed from the solution in NAV/Business Central. It is the customers responsibility to manage user from within NAV/Business Central and synchronize with Continia Online Services.

General approval Data (except PDF-files and attachments) related to documents for approval are stored in the cache of the current user and removed when the session of the user expires.

PDF-files and attachments will be stored for 4 hours and removed afterward.

3. Content
Data related to allowed users. Such as Dynamics NAV/Business Central username, Windows username, E-mail address, Full name

General approval data related to documents for approval. Such as purchase invoice header and line information, expenses, list of required approvers, approval comments, etc.

PDF-files and attachments: depend on the content of PDF-files and attachments. Typically, at least a copy of the purchase invoice.

4. Sensitivity
Personal data of the users are considered less sensitive.

The content of approval Data, PDF-files and attachments are considered potentially personal sensitive, but beyond the control or influence of Continia.

2.4.4. Personal Data related to Continia Payment Management

When using Payment Management The Customer (its users) can create, send and retrieve payment files.

This is accomplished with the use of two external components (dll-files), meaning they are not part of the Microsoft Dynamics NAV/Business Central software package, but delivered by Continia Software:

1. The Continia Bank Integration Component (CBIC) for creating the file, and

2. The Continia Bank Communication Component (CBCC) for sending the file to the bank and for retrieving status files, inpayment files and account statements.

In Payment Management however, the user has the choice to either:

1. Install and use the Continia Bank Integration Component (CBIC) locally, or

2. Use the Continia Bank Integration Component (CBIC) on Continia Online.

The Continia Bank Communication Component (CBCC) is always installed locally.

Depending on your settings above, only Continia Online-installed components is Continia Software's responsibility and therefore relevant for this documentation. Locally installed components, or files saved to a local file-location, is the responsibility of the user.

1. Flow

Creating the payment file:

When creating payments with Payment Management, an xml-formatted file is created with payment Data from Dynamics NAV/Business Central. The file is then sent to the CBIC component, installed locally or using the Continia Online version.

The CBIC component then process the payment Data in the xml-formatted file and creates a new xml-formatted file that fits with the chosen banks file format. The new file is then sent back to Dynamics NAV/Business Central.

Sending the payment file:

When sending payments with Payment Management, (the payment file returned by the CBIC component), depending on which setting the user have selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, the payment file generated by the CBIC will be sent to the locally installed CBCC component, which will handle the communication with the bank using the users Certificate.

2. If the user has selected Manuel Communication, the payment file generated by the CBIC is saved on a user-specific file location. The user must then manually upload the file to the bank either using a SFTP-folder or using the banks online system, which will handle the communication with the bank.

Retrieving status files, inpayment files and account statements:

When receiving status files, inpayment files and account statements with Payment Management, depending on which setting the user have selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, the Dynamic NAV/Business Central will generate a request file and send the file to the locally installed CBCC, which will handle the communication with the bank using the user's Certificate. Based on the request-file the CBCC component then retrieves the files requested and send the files back to Dynamics NAV/Business Central.

2. If the user has selected Manuel Communication, the files must be manually downloaded, for example using the banks online system, and afterwards imported into Dynamics

NAV/Business Central using Payment Management feature-specific import actions.

2. Expiration

Using Continia Bank Integration Component (CBIC):

Creating the payment file: Data are not saved locally and they expire immediately after the generated xml file is sent back to Dynamics NAV/Business Central.

Using Continia Bank Communication Component (CBCC):

Creating Certificate: Data are not saved locally and they expire immediately after the certificate is sent to the bank and secure communication has been established.

Sending the payment file: Data are not saved locally and they expire immediately after the file is sent to the bank.

Retrieving status files, inpayment files and account statements: Data are not saved locally and they expire immediately after the retrieved files is send to Dynamics NAV/Business Central.

3. Content

Data related to Creating and Sending Payment file:

Sender such as Bank Reg. No., Account No., Address, CVR, CPR, Amount, Company Name, Company Address, Currency, Bank Name, Bank IBAN, Bank SWIFT, Sender reference.

Recipient such as Name, Address, Account No. Account Reg. No., Bank Name, Bank IBAN, Bank SWIFT, Creditor Number, SE-No., P-No., Receiver Reference.

Creating Certificate such as Sender-id, Signer-id, Receiver-id, Certificate-holder, activation-code.

Data related to Retrieving status files, inpayment files and account statements Such as
Bank user information, File reference number from bank, Swift number, IBAN.

4. Sensitivity

All Data are considered confidential but not sensitive personal data.

2.4.5. Personal Data related to Continia Payment Management 365

When using Continia Payment Management 365 you can create, send and retrieve payment files.
This is accomplished with the use of two external components installed on Continia Online, meaning they are not part of the Dynamics 365 Business Central software package, but delivered by Continia Software.

1. The Continia Bank Integration Component (CBIC) for creating the file, and

2. The Continia Bank Communication Component (CBCC) for sending the file to the bank and for retrieving status files, inpayment files and account statements.

Locally installed components, or files saved to a local file-location, are the responsibility of the user.

1. Flow

Creating the payment file:

When creating payments with Payment Management 365, an xml-formatted file is created with payment data from Dynamics 365 Business Central. The file is then sent to the CBIC component on Continia Online.

The CBIC component then process the payment data in the xml-formatted file and creates a new xml-formatted file that fits with the chosen banks file format. The new file is then sent back to Dynamics 365 Business Central.

Sending the payment file:

When sending payments with Payment Management 365, (the payment file returned by the CBIC component), depending on which setting the user have selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, the payment file generated by the CBIC will be sent to the CBCC component on Continia Online, which will handle the communication with the bank using the user's Certificate.

2. If the user has selected Manuel Communication, the payment file generated by the CBIC is saved on a user-specific file location. The user must then manually upload the file to the bank either using a SFTP-folder or using the bank's online system, which will handle the communication with the bank.

Retrieving status files, inpayment files and account statements:

When receiving status files, inpayment files and account statements with Payment Management 365, depending on which setting the user has selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, Dynamics 365 Business Central generates a request file and sends the file to the CBCC component on Continia Online, which will handle the communication with the bank using the user's Certificate. Based on the request-file the CBCC component then retrieves the files requested and send the files back to Dynamics 365 Business Central.

2. If the user has selected Manuel Communication, the files must be manually downloaded, for example using the banks online system, and afterwards imported into Dynamics 365 Business Central using Payment Management 365 feature-specific import actions.

2. Expiration

Using Continia Bank Integration Component (CBIC):

Creating the payment file: Data are not saved locally and they expire immediately after the generated xml file is sent back to Dynamics 365 Business Central.

Using Continia Bank Communication Component (CBCC):

Creating Certificate: Data are not saved locally and they expire immediately after the certificate is sent to the bank and secure communication has been established.

Sending the payment file: Data are not saved locally and they expire immediately after the file is sent to the bank.

Retrieving status files, inpayment files and account statements: Data are not saved locally and they expire immedietly after the rectreived files is sent to Dynamics 365 Business Central.

3. Content

Data related to Creating and Sending Payment file:

Sender such as Bank Reg. No., Account No., Address, CVR, CPR, Amount, Company Name, Company Address, Currency, Bank Name, Bank IBAN, Bank SWIFT, Sender reference.

Recipient such as Name, Address, Account No. Account Reg. No., Bank Name, Bank IBAN, Bank SWIFT, Creditor Number, SE-No., P-No., Receiver Reference.

Creating Certificate such as Sender-id, Signer-id, Receiver-id, Certificate-holder, activation-code.

Data related to Retrieving status files, inpayment files and account statements Such as

Bank user information, File reference number from bank, Swift number, IBAN.

4. Sensitivity -

All data are considered confidential but not sensitive personal data.

2.4.6. Personal Data related to Continia MobilePay 365

When using Continia MobilePay 365 The Customer can create and send collection request to MobilePay Denmark and retrieve status files. This communication is established using Continia Online components.

During communication to MobilePay Denmark, the Customer's MobilePay Business Credentials will be sent to Continia Online. These MobilePay Business Credentials are necessary because the Continia Online component needs to check that the MobilePay Business Credentials are valid, before making any MobilePay collections.

Customer Data will be sent to Continia Online as a part of the collection request.

1. Flow

When installing the Continia MobilePay 365 extension on Dynamics 365 Business Central the user will be asked to enter the MobilePay Business Credentials. This happens as a part of the initial configuration of the extension.

2. Expiration

Business Credentials: MobilePay Business Credentials will be sent to Continia Online when creating a collection request, as soon as the Business Credentials has been validated they will expire on Continia online.

Customer Data: Customer data will be sent to Continia Online as a part of the collection request. The collection request and the related data will not be saved on contina online and expires when the request is sent to MobilePay.

Status files: Callbacks from MobilePay will contain information about the collection request and the Customer. Callbacks will be stored on Continia online until they are collected by Continia MobilePay 365 on Dynamics 365 Business Central. If callbacks are not collected they will be stored for a maximum of 180 days at which time they will automatically be deleted.

3. Content

Credentials: Credentials for MobilePay Business.

Customer Data: Name, E-mail, Phone No., Amount.

Callback Data: Name, E-mail, Phone No., Amount.

4. Sensitivity
All Data are considered confidential but not personal sensitive.

2.4.7. Data Related to Continia MobilePay Invoice

When using MobilePay Invoice the Customer (and its users) can create and send invoices as a request for payment to MobilePay Denmark A/S and retrieve status answers and inpayment files.

This is accomplished with the use of an external component installed on Continia Online, meaning it is not part of the Microsoft Dynamics 365 Business Central software package, but delivered by Continia:

1. The Continia MobilePay Interface Component.

Below is a description of how MobilePay Invoice communicates with Continia Online.

1. Flow
Creating the invoice request: When creating an invoice request with MobilePay Invoice, a json-formatted request is created with Data from Business Central. The request is then sent via a secure https-protocol to the Continia MobilePay Interface Component on Continia Online.

The Continia MobilePay Interface Component then sends the request to MobilePays API.

Sending the invoice request: When sending invoice request with MobilePay Invoice, the following flow is used:

1. If the user has selected InvoiceDirect, the invoice request generated by the Continia MobilePay Interface Component is sent to the MobilePay Portal using the OpenID Certified certification process.

2. If the user has selected InvoiceLink, the invoice request generated by the Continia MobilePay Interface Component is sent to the MobilePay Portal using the OpenID Certified certification process. The MobilePay Portal then creates a Link which is returned to the Continia MobilePay Interface Component and embedded in the invoice and invoice request.

Retrieving status on invoices: States for the MobilePay Invoices will be sent to Continia Online from MobilePay, they will then await a request from MobilePay Invoice to import the new states of all active payments.

2. Expiration
Using MobilePay Invoice:

Sign-up: when signing up, data is stored at Continia Online to enable communication with MobilePay.

Sending invoices: When sending invoices, data is stored at Continia Online.

Retrieving States: When States of Invoices is imported to MobilePay Invoice, data will be stored at Continia Online.

3. Content
Data related to Creating and Sending Payment file:

Sign-up: Merchant Id, Client ID, API key, is merchant id registered with another company on Continia Online.

Sender Such as Business Central Invoice Id, MobilePay Invoice ID, AccessToken, RefreshToken, Callback url, status.

Data related to Retrieving status on payments:

Error code, error message, Invoice callback id, redirect url for payment.

4. Sensitivity
All data is considered confidential but not personal sensitive.

2.4.8. Data related to Continia Mobilepay 365 Subscription

When using MobilePay Subscriptions the Customer can create and send payment agreements and one-off payments as a request for payment to MobilePay Denmark A/S and retrieve status, answers, inpayment files and automatically collect payments as long as the payment agreement is active.

This is accomplished with the use of an external component installed on Continia Online, meaning it is not part of the Microsoft Dynamics 365 Business Central software package, but delivered by Continia:

1. The Continia MobilePay Interface Component.

Below is a description of how MobilePay Subscriptions communicates with Continia Online.

1. Flow
Creating the Payment agreement and One-off payment request: When creating a payment agreement or one-off payment request with MobilePay Subscriptions, a json-formatted request is created with data from Business Central. The request is then send via a secure https-protocol to the Continia MobilePay Interface Component on Continia Online.

The Continia MobilePay Interface Component then sends the request to MobilePays API.

Sending the Payment Agreement request: When sending Payment agreement request with MobilePay Subscriptions, the following flow is used:

1. The payment agreement request generated by the MobilePay Subscriptions Extension is sent to the MobilePay Portal using Continia Online.

2. The MobilePay Portal creates a Link which is returned to the Continia MobilePay Interface Component, which is returned to Business Central and then used to either send to customer or open inside Business Central and send the payment agreement request directly to the customers mobile phone.

Retrieving status on payment agreements:States for the MobilePay payment agreement will be sent to Continia Online from MobilePay, Continia Online will then await a request from MobilePay Subscriptions to import the new states of all active payment.

Sending payments: When creating a payment on an existing MobilePay Subscriptions agreement, the following flow is used:

The One-off payment request generated by MobilePay Subscriptions Extension is sent to Continia Online which sends the request to the MobilePay Portal. The MobilePay Portal then creates a Link which is returned to Continia MobilePay Interface Component, which is returned to Business Central where users are able to open the link in Business Central or send it to the Customer for activating the One-off payment so it appears in their MobilePay app.

Recurring payment request generated by the MobilePay Subscriptions Extension is sent to Continia Online which send the request to the MobilePay Portal. The payment will be collected unless the Customer cancels it.

Retrieving status on payments:States for the MobilePay One-off payments will be sent to Continia Online from MobilePay, Continia Online will then await a request from MobilePay Subscriptions to import the new states of all active One-off payments.

Sates for the MobilePay recurring payments will be sent to Continia Online from MobilePay, Continia Online will then await a request from MobilePay Subscriptions to import the new states of all recurring payments.

2. Expiration
Using MobilePay Subscriptions:

Sign-up: when signing up, Data are stored at Continia Online to enable communication with MobilePay.

Sending payment agreements: when sending payment agreements, Data are stored at Continia Online.

Retrieving States: When States of payment agreements are imported to MobilePay Subscriptions, data will be stored at Continia Online.

3. Content
Data related to Creating and Sending payment agreement:

Sign-up: Merchant Id, Client ID, Company GUID, AccessToken and RefreshToken, whether the merchant id registered with another company on Continia Online.

Callbacks: Provider Id, API key, configured callback urls.

Data related to Retrieving status on payment agreements:

AgreementId, internal id, transactionid, timestamp, Status_code, Status_text and Status.

4. Sensitivity
All data is considered confidential but not personal sensitive.

ANNEX III

3. 1. Measures regarding security of processing

The processor shall primarily assist the controller in ensuring an adequate level of processing security, in accordance with Article 32 GDPR as well as Clause 7.4. by implementing technical and organisational measures to establish the necessary level of data security.

Please see the attached Information Security Manual and latest ISAE 3402 Type II Assurance Report performed by an independent auditor regarding the implemented technical and organisational measures.

3.2. Direct Assistance to the Controller

The processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the controller directly in accordance with Clause 8 by the following:

(a) The processor shall upon request make the necessary information available to the controller necessary for the controller to comply with Clause 8.

(b) If necessary, the processor shall assist the controller in identifying the relevant personal data in connection with the fulfilment of the controller's obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR.

(c) If necessary, the processor shall - in the form of technical or organisational measures - assist the controller in observing requests for rectification or deletion in accordance with Articles 16 and 17 GDPR.

Any costs incurred by the Processor in connection with the above stated assistance will be payable by the Controller pursuant to an agreed fee scheme.

3.3. Procedures for the controller's audits, including inspections, of the processing of personal data being performed by the processor

The controller or the controller's representative shall have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the processor, including physical facilities as well as systems used for and related to the processing.

Such an inspection shall be performed, when the controller has assessed and determined that the current certifications held by the processor are insufficient and has duly informed the processor in writing.

Any inspection or audit must be notified by the controller to the processor with at least 1 month notice and all costs incurred by the processor are payable by the controller.

The processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

3.4. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The processor shall, on the basis of an assessment of the risks to the rights and freedoms of the data subjects related to the specific processing activities to be carried out by sub-processor, determine how the processor will audit sub-processors' compliance with the GDPR, the applicable

EU or Member State data protection provisions and any Clauses which the processor has agreed with the sub-processor.

Further, the processor shall determine how often and to what extent the processor will audit those sub-processors and implement these audits in the processors technical and organizational measures to ensure that those sub-processors comply with the GDPR, the applicable EU or Member State data protection provisions and any Clauses which the data processor has agreed with the sub-processor.

3.4. Procedure for assessing and implementing measures derived from subsequent instructions from the controller to the processor

The controller has, as stated in Clause 7.1, the right to issue subsequent instructions to the processor throughout the duration of the processing of personal data. In such an event the controller must convey these instructions to the processor by either contacting the processors contact person as stated in Annex I or contact the processor through dpo@continia.com.

The processor will then assess the received instructions in order to determine whether the processor is able or willing to implement the measures contained in the subsequent instruction. The processor will implement measures that are required by Union law or Member State law to which the processor is subject within a reasonable time frame.

The processor however retains the right to refuse implementing instructions that the processor either deem to exceed measures required by Union law or Member State law to which the processor is subject,or are based on requirements that originate from third country legislation.

In any such event as described above or in the event that the provisions of Clause 10 for whatever reason becomes applicable and the controller decides to terminate the contract between the controller and the processor the conditions of termination stated in the Main Agreement will apply.

ANNEX IV

List of sub-processors

The controller has authorised the use of the following sub-processors:

Name: Microsoft: Ireland Operations Ltd.

Address: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland

Description of the processing: The provided service is Azure Cloud Service which is used by Processor as the cloud storage facility and operating environment of its current online services.

Country of processing: Ireland

Name: ABBYY Europe GmbH

Address: Landsberger Str. 300 80687 Munich, Germany

Description of the processing: The provided service is Cloud OCR Service which is part of the Processor's Document Capture product see Annex II for further details of the specific processing.

Country of processing: The Netherlands

Name: Amazon Web Services EMEA SARL

Address: 38 Avenue John F. Kennedy, L-1855 Luxembourg

Description of the processing: The provided service is an e-mail service which is part of the Processor's Document Capture product, see Annex II for further details of the specific processing.

Country of processing: Ireland

Name: Tickstar AB

Address: Triewaldsgränd 2, SE-111 29 Stockholm, Sweden

Description of the processing: The provided service is an access point functionality for the PEPPOL network, which is part of the Processor's Delivery Network product.

Country of processing: Ireland